OIPE IAP58
JAN 3 1 2006
PATENT & TRADEMARK OFFICE

Appl. No. 10/082,235
Response Dated January 27, 2006
Reply to Office Action Dated October 27, 2005
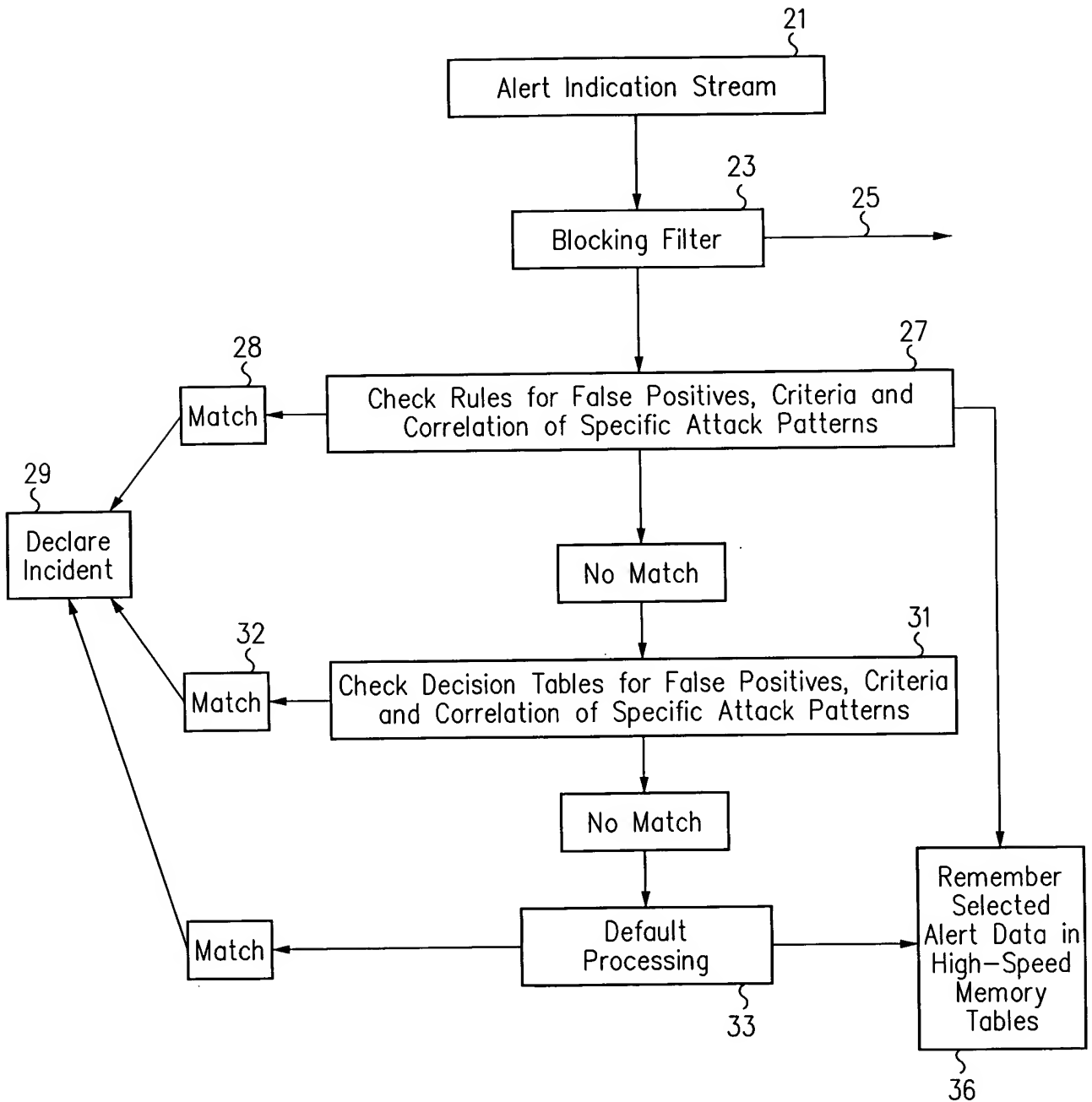Replacement Sheet

1/5

FIG. 1
(PRIOR ART)

FIG. 2
(PRIOR ART)

Appl. No. 10/082,235
Response Dated January 27, 2006
Reply to Office Action Dated October 27, 2005
Replacement Sheet

2/5

21

Alert Indication Stream

23

Blocking Filter → 25

28

Match ← 27

Check Rules for False Positives, Criteria and Correlation of Specific Attack Patterns

29

Declare Incident

No Match

32

Match ← 31

Check Decision Tables for False Positives, Criteria and Correlation of Specific Attack Patterns

No Match

Match ← Default Processing → Remember Selected Alert Data in High-Speed Memory Tables

33

36

FIG. 3

Appl. No. 10/082,235
Response Dated January 27, 2006
Reply to Office Action Dated October 27, 2005
Replacement Sheet

3/5

OIPE JAN 3 1 2006 PATENT & TRADEMARK OFFICE

CyberWolf Incident Ticket—Microsoft Internet Explorer

File Edit View Favorites Tools Help

CyberWolf

Incident Ticket	ID: 1012 Status: Open Priority: Critical

Update Tracking Criteria	Update Incident	Check History	Help

INCIDENT DESCRIPTION

"An attempt to send a binary shellcode to a host has been detected. This could indicate an attempt to execute a buffer overflow attack and gain unauthorized access to system resources."–AlertType–OS_MultiVendor_noop TrackingSource–10.193.111.87 TrackingTarget–10.193.111.4 Category–OSExploits ExpertType–SnortExpertSeverity–1

Date Time	CONCLUSIONS
13: 45 02/22/02	"An attempt to send a binary shellcode to a host has been detected. This could indicate an attempt to execute a buffer overflow attack and gain unauthorized access to system resources." –AlertType–OS_MultiVendor_noop TrackingSource–10.193.111.87 TrackingTarget–10.193.111.4 Category–OSExploits ExpertType–SnortExpertSeverity–1
13: 45 02/22/02	"An HTML file has been modified on the Web server."–AlertType–HTMLFileModify TrackingSource–10.193.111.87 TrackingTarget–10.193.111.87 DeviceIP–10.193.111.87 Category–FileSystemAccess TargetFile–/home/httpd/html/_HomePage.htm ExpertType–ApacheExpert Severity–1
13: 45 02/22/02	"An attempt to log in to the host as root failed because the user entered an invalid password or attempted to log in from a remote terminal.""AlertType–RootLoginAuthFailure TrackingSource–10.193.111.87 TrackingTarget–10.193.11.87 Category–AuthenticationViolations ExpertType–LinuxExpert Severity–
13: 45 02/22/02	Unauthorized Access Attempt detected on an asset that was recently port scanned – Last scan ocurred 1 seconds previous to following alert – "An FTP connection to the host was refused."–AlertType–FTPRefused TrackingSource–10.193.111.48 TrackingTarget–10.193.11.87 Category–AuthenticationViolations ExpertType–LinuxExpert Severity–3

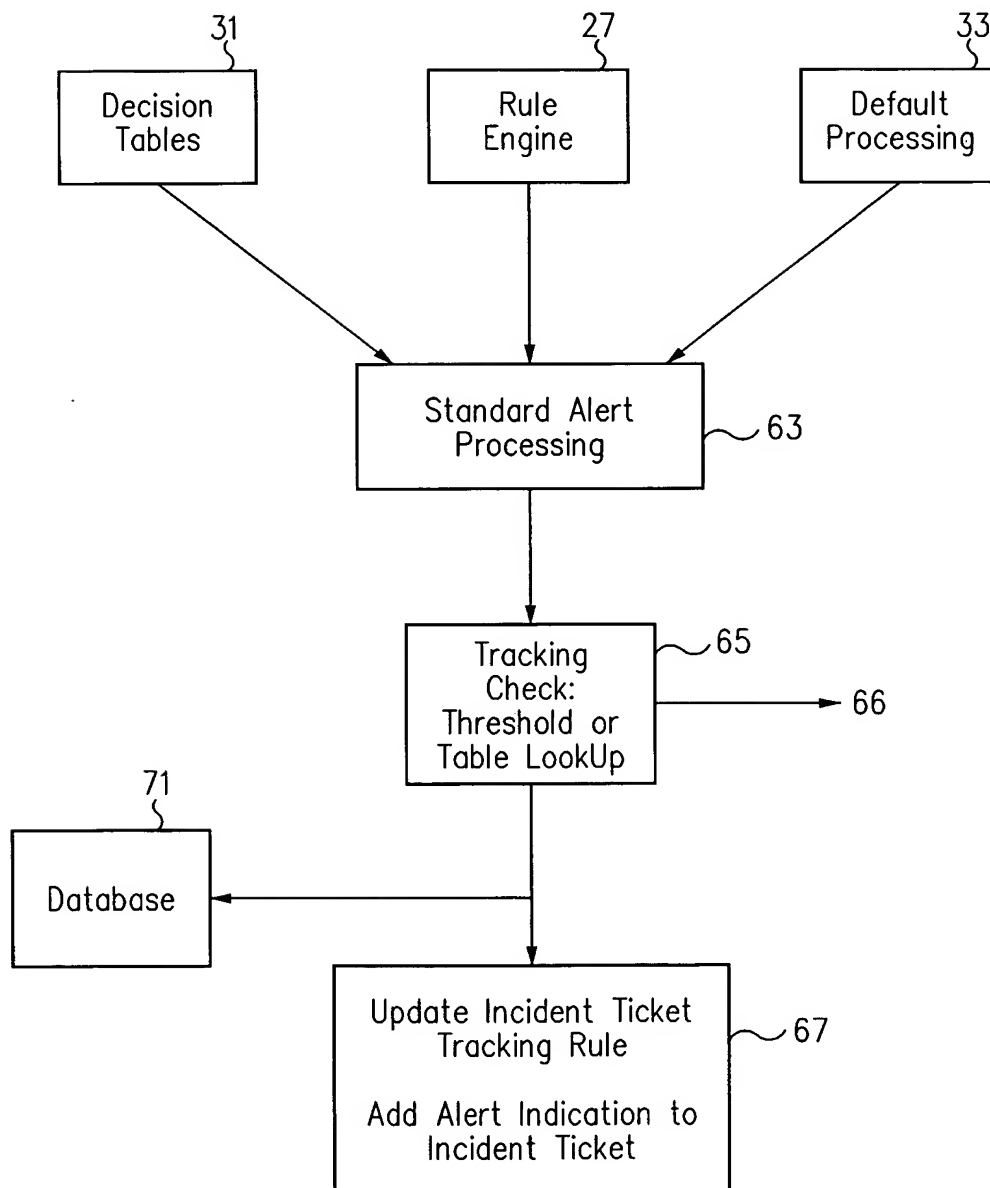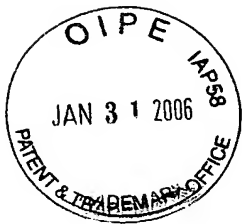| Date Time	Agent	ACTIONS
Tracking Rule		
Source:	10.193.111.48	
Targets:	10.193.111.87	10.193.111.4
User Rule	And {TargetPort} Is "2033"	
Date Time	ALERTS	
13: 45 02/22/02	Description "An attempt to send a binary shellcode to a host has been detected. This could indicate an attempt to execute a buffer overflow attack and gain unauthorized access to system resources."FromLogSim0 SeverityISourceIP TargetIP 10.193.111.4 GenericAlert OS_MultiVendor_noop	

Done   Internet

FIG. 4

Appl. No. 10/082,235
Response Dated January 27, 2006
Reply to Office Action Dated October 27, 2005
Replacement Sheet

4/5

```
  ┌──────────┐      ┌──────────┐      ┌──────────┐
  │   31     │      │   27     │      │   33     │
  │ Decision │      │   Rule   │      │ Default  │
  │  Tables  │      │  Engine  │      │Processing│
  └────┬─────┘      └────┬─────┘      └────┬─────┘
       └────────────┐    │    ┌────────────┘
                    ▼    ▼    ▼
              ┌──────────────────┐
              │  Standard Alert  │ ── 63
              │    Processing    │
              └────────┬─────────┘
                       │
                       ▼
              ┌──────────────────┐ ── 65
              │     Tracking     │
              │      Check:      │────────► 66
              │   Threshold or   │
              │   Table LookUp   │
              └────────┬─────────┘
   ┌──────────┐        │
   │   71     │        │
   │ Database │◄───────┤
   └──────────┘        │
                       ▼
              ┌──────────────────────┐
              │ Update Incident Ticket│ ── 67
              │    Tracking Rule     │
              │                      │
              │ Add Alert Indication to│
              │    Incident Ticket   │
              └──────────────────────┘
```

FIG. 5

Appl. No. 10/082,235
Response Dated January 27, 2006
Reply to Office Action Dated October 27, 2005
Replacement Sheet

5/5

CyberWolf Tracking Criteria–Microsoft Internet Explorer	— □ ✕

File Edit View Favorites Tools Help

CyberWolf

Update Tracking Criteria | Incident#1012

☐ Disable Auto Update of Tracking Rule   ☑ Show Details

| Source: | 10.193.111.48 |
| Targets: | ☑ 10.193.111.87   ☑ 10.193.111.4 |

Select All   Unselect All

	And/Or	(	Attribute Name	Condition	Attribute Value	)
INS / DEL	And ▼	▼	TargetPort ▼	Is ▼	2033 ▼	▼
INS / DEL	▼	▼	▼	▼	▼	▼

Submit   Reset   Help

Done   🔒 🌐 Internet

77   71   73   75

70

FIG. 6